IN THE CLAIMS

Please amend the claims as follows:

Claims 1-23 (Canceled).

Claim 24 (Currently Amended): A computer-implemented method of encrypting plural variables and mapping components of multivariate mappings, represented, with univariate mappings of an appropriate representation, comprising the steps of:

A. determining a representation for the encryption;

B. replacing each variable to be decrypted x_i with a decrypted equivalent $s_{e+i}(x_i)$;

C. composing the decrypted equivalents with a mapping h; and

D. composing each mapping component to be encrypted, h_i, with an encryption function r_i, to create $r_i(h_i(\ldots))$.

Claim 25 (Original): The method as claimed in claim 24, wherein the multivariate mappings comprise mappings represented as one of function tables and polynomials.

Claims 26-33 (Canceled).

Claim 34 (Currently Amended): A computer-implemented method of generating keys for multivariate encryption of multivariate mappings, comprising the steps of:

A. determining a representation for the keys including key triples;

B. defining a polynomial f to translate from base-N vectors having c_i components to base-N^{c_i} numbers;

[[B.]]C. defining, for an i^th key triple ~~two temporary~~ , arrays R_i and S_i each having $N^{c_i} \times (c_i + 1)$ ~~arrays R and S~~ elements;

~~C. defining a temporary polynomial f to translate from base N vectors to base N^{c_i} vectors with c_i components; and~~

D. permuting a ring $Z_{N^{c_i}}$, and simultaneously translating a permutation and its inverse to a field $Z_N^{c_i}$ ~~for every key triple~~, storing ring permutations in R_i and storing translated permutations and inverses in S_i;

E. repeating steps B-D for ~~all triples~~ each key triple not set equal to identity; and

F. converting each array R_i and S_i to the determined key representation.

Claim 35 (Original): The method as claimed in claim 34, wherein the mappings to be encrypted are expressed using polynomials, further comprising the step of computing the permutation and its inverse by interpolation, using at least a portion of R and S as interpolation data, using $a_i(x)$, once for each unique key triple that is to be generated.

Claim 36 (Original): The method as claimed in claim 34, further comprising the step of setting all key triples that are to do neither encryption nor decryption to the identity mapping.

Claim 37 (Original): The method as claimed in claim 34, further comprising the steps of (1) pre-computing arithmetic operations over the field Z_N and (2) pre-computing coefficients of the functions $a_j(x)$, wherein the steps of permuting comprises using the pre-computed $a_j(x)$.

Claim 38 (Original): The method as claimed in claim 34, further comprising the step of restricting a new set of key triples based on a pattern of encryption used during an encryption of the first multivariate polynomials.

Claim 39 (Currently Amended): A computer-implemented method of encrypting plural groups of variables and groups of mapping components of multivariate mappings, with other multivariate mappings, comprising the steps of:

A. determining a mapping representation for encryption;

B. replacing each group of encrypted variables $\vec{w}_i$ with a decrypted equivalent $s_{i+l}(\vec{w}_i)$;

C. composing each of the decrypted equivalents with a mapping h; and

D. composing each group of mapping components to be encrypted v_i with r_i giving $r_i(v_i(\ldots))$.

Claims 40-67 (Canceled).